Cybersecurity Implications of the Russia-Ukraine Conflict

29 March 2022 – Middlesex University, Mauritius

Amar Seeam
Okay, good morning, everyone. Thanks for joining us today for this hybrid webinar. Let me introduce myself. For those who don't know me, I'm Amar Seeam. I'm a lecturer at Middlesex University Mauritius. I teach a number of topics related to cybersecurity Internet technologies, virtualization network management, so I'm very interested in hearing more about today's topic. Or Today also marks an interesting day for our campus. We are launching the IEEE Middlesex University of Mauritius student branch so this is the first branch that we've have on the island, and it's the first for a branch, campus and Mauritius. And we're gonna kick off with a series of webinar events and activities, which are here more of a from the branch itself and a few moments. And so we've kicked off today with quite an interesting topic. You may have heard in the news, some of the more severe cyber attacks in the conflict and Ukraine to be affected quite severely and our guest speaker is going to be talking more about that in a few moments. I'm now going to pass it on to our Chair of the organization who wishes to talk more about the branch and to introduce our guest

Elnathan Vally

Thank you. Good morning everyone, to represent myself, my name's Elnathan, and I'm the chairperson and founder of the IEEE Middlesex University Moshe student lunch so just a short definition of what is IEEE? IEEE is Institute of Electrical, Electrical and Electronic Engineers. It is one of the world's largest professional organization that is dedicated to advancing technology for the benefit of humanity. IEEE's members inspire global community through its highly cited standards, publications, conferences, and professional and educational activities. Our aims and objectives of the branch is to meet and learn from IEEE guides and graduate student members and engage with professional IEEE members. An active IEEE student branch can be one of the most [inaudible] of one's academic career, offering programs activities and professional networking. opportunities that build critical skills outside the classroom. IEEE has student branches in 1000s of university worldwide, and here in Mauritius we have three active branches, there is one at the University of Mauritius, one at the University of Technology, and here one at Middlesex University. We aim at organizing competitions, hackathons, as well as we call international conferences and workshops, like the one we're having today, that is a hybrid webinar.

Elnathan Vally
So I will introduce to you about the speaker. The speaker is Dr. Amreesh Phokeer from the Internet Society, and has joined Internet Society as Internet Measurements and Data Expert in 2021. He's focused on research around Internet measurement, Internet shutdowns, and understanding market trends that impact the growth of Internet across the globe. Prior to joining ISOC, Amreesh was a research manager at the African Network Information Center, AFRINIC, where he spearheaded organization research activities in the areas of Internet security and Internet measurement. Amreesh has an MSc in information security from Royal Holloway University of London and a PhD in computer science from the University of Capetown, South Africa. So, I will now leave the floor to Amreesh Phokeer, who will lead on with the hybrid webinar.

Amreesh Phokeer
Good morning, everyone. Students, lecturers. Thank you for the kind invitation and I'm glad to be here. Glad to be back at the university. I did some projects with master students I think two years ago before COVID breaks, but I'm glad to be back. I hope to renew the experience sometime soon. So my name is Amreesh Phokeer. I work for the Internet Society. And today my talk is going to be about cyber security implications of the Russia Ukraine conflict. I crossed out security because I'm going to talk more generally about the cyber implications. So let's start.

Well, you already give a very good introduction. I joined the Internet Society, which is a global nonprofit, since last year working on different projects, including Measuring the Internet, so understanding the health of the Internet from different aspects, whether we are adopting the

newest best practices, the newest technologies, what are the impediments, so on and so forth? I do a lot in what we call routing security. We have that protocol called the Border Gateway Protocol, which has a lot of security flaws. And we try to inform network operators how to improve the security through different security mechanisms.

I'm also involved in what we call Internet peering. We'll see why peering is important. Peering is about having network operators get together and exchange traffic in a more efficient and less costly way, and we try to as much as possible to encourage people to adopt the peering and Interconnection best practices.

I'm also involved very recently in what we call the LEO project, Low Earth Orbit satellites. You must have heard about Starlink. The Internet Society is currently investigating about, what are the benefits or the drawbacks of Starlink, because as you know there are there are many benefits to to the the low earth orbit project because it can bring Internet access to areas where it is usually difficult to provide access, but at the same time it creates a lot of pollution in the space and things like that. So, all those things we are currently researching, and probably soon we will have a position on this project -- on this technology, rather.

I worked at AFRINIC before as a research manager for almost 10 years on very similar topics, but mostly focusing on the African networks. I'm also involved in a lot in the academic community, I participate in as the as the technical program committee member at a few conferences such as the Internet Measurement Conference, Passive and Active Measurement Conference, and TMA. I also had the chance to work with Amar a few years ago to organize the AFRICOMM 2020, which we did together with the Middlesex. Unfortunately, it was it was virtual, but nonetheless I think it was a good event.

So, back to the Internet Society. I mentioned we are a global NGO. We were founded in 1992 by the Internet pioneers. You might have heard of Vinton Cerf, who is the inventor of the TCP/IP. So, all these people at the beginning said that, Okay, why don't we create a nonprofit that will impart all the good things of the Internet, and also make sure that we work in such a way that we keep the Internet open and accessible to everyone, and also using the latest and the best technologies out there. So, our motto is, We stand for a better Internet. We have a global presence of a community of members. We have individual members, anyone can become a member of the Internet Society, and we have also corporate members, and our strength really is in the network of Chapters. We have chapters in in many, many countries. We had a chapter in Mauritius, but unfortunately it went dormant, so maybe I would encourage you to find some information, I would gladly help you, to how to rejuvenate this chapter, and benefit from all the activities that the

Internet Society organizes, from providing grants to providing training on technical or less technical aspects of the Internet. If you want to do research, you can apply for grants. You can also become what we call an Early Career Fellow, where we would give you some training, and allow you to meet industry leaders like Vinton Cerf, who is participating in this program to establish some sort of interaction, so I would really encourage you to participate.

So what do we do? As I mentioned, at the Internet Society we provide leadership in policy issues. Policy could be, let's say, a country is doing an Internet shutdown. We would write some policy briefs to say, what are the drawbacks of doing an Internet shutdown? For example, it is cutting access to the Internet, a lot of people, especially in developing regions, they rely on the Internet for their day-to-day business. For example, someone working in the informal sector might be using WhatsApp for their day-to-day business. This is important for them, so if you cut Internet access, you might be cutting the access to their funding, and this can have dire consequences.

We advocate for an open Internet, based on Internet standards. As you know, the Internet is based on Internet protocols which are open, and which anybody can contribute to, and which is also openly accessible. So, as much as possible, we want to keep the Internet open through open technologies. We promote Internet technologies that matter. For example, switching to ipv6 is an important move that we must do, as IPv4 is depleting. We must, for example, protect the DNS system by adding a security layer called DNSSEC. These sort of technologies.

We develop infrastructure, so we have built technical community in the different countries. For example, in Mauritius, we had built a Mauritius Internet exchange point. As I mentioned, an exchange point is an important infrastructure which allows operators to connect to each other, because otherwise what would happen? They would need to connect to a foreign operator, send traffic outside of Mauritius for the traffic did come back to Mauritius. The Internet exchange point allows better interconnection within the country.

Then we finally also recognize industry leaders. We have what we call the Jon Postel award. Jon Postel is also one of the pioneers. We give awards to people who are doing good things, promoting the openness of the Internet or building infrastructure in their communities.

Back to our talk today. I thought this talk would be quite timely, because we are right amid a war, unfortunately. We at the Internet Society do not condone any sort of violence, and we know that this war is being very violent, people cannot leave the house, sometimes even at the expense of their life. So, what's happening in Ukraine is bad, and we provide our full support to the Ukrainian community.

Here is just a summary of cyber events that happened. As you know, Russia invaded Ukraine in on the 24th of February, and this after building up a lot of military forces for several months. But, at the same time, you would be interested to know that they have also conducted cyber attacks on countries such as the NATO countries and their allies, and I would say the whole game was actually to control the information flow, to control the pipelines, trying to cut Internet in some regions, and also disrupt the information flow, and try to propagate fake news, because this is part of the new way of doing war, basically.

There have been various techniques, multiple known and unknown attack vectors were used, for example ransomware, as you know, wiperware was used a lot. So, data leaks and cyber espionage. Data leaks? You would see that the attacks are coming from both sides, the Ukrainians are also retaliating. Very recently, I think yesterday, or two days ago, the anonymous group released a statement saying that they have released 28 gigabytes of worth of data of the Central Bank of Russia. So it's out, public, you have so many information on contracts and deals and everything involved. Maybe one landmark event that happened is that the EU and the US also put sanctions on Russia, and also on the Russian Internet. We will see later elaborate on this.

One of the first thing that we decided to do at the Internet Society is to see how resilient the Ukrainian Internet is. The war has been going on for a month now, but we haven't heard about big outages in Ukraine. And that's true. Of course, they have started to bombard buildings hosting data centers, which is breaking Internet in some parts of the of the country, but, in general, the Ukrainian Internet has been quite resilient. This is thanks to the very good infrastructure that they had right at the beginning. As you can see on the map, it is the cable infrastructure which covers most of the country, and all the orange dots are the exit points, because, let's say, if a few exit points are controlled by the Russian authorities or military, the other exit points are still accessible for them to send traffic out of the country, and receive traffic from other networks.

But, on top of that, they have a very strong infrastructure itself in terms of Internet exchange points, for example. I was talking about those infrastructures that allow operators to connect to each other and exchange traffic locally. They have 20 of these for Ukraine. They have more than 50 data centers, and more than 30 network operators, so Internet Service Providers. That's good, because the more diverse your market is, so it means that you have a low market concentration, it is more difficult to shut down the whole of the Internet of Ukraine, because it is so diverse, it is so well connected to every different places. This is a good example that many countries need to follow.

Market concentration, if we take the example of Mauritius, not to bad name anyone, but our incumbent operator controls 75% of the market, and 20% goes to the other operators. The thing is, what happens in, let's say, Mauritius Telecom has a cable break? Which happens in many countries. So, it might so happen that 75% of the population will not have access to the Internet. So, the more variety we have, the more diversity we have, it's better in general.

So far it has been good, but yesterday the Ukraine Telecom connectivity dropped because of cyber-attacks. So, this is now happening. They hit their routing infrastructure, so for a lot of their customers, Internet was not accessible anymore. As I mentioned, in the areas of fighting there are regional and localized outages. I have even seen pictures of people, after their building being bombarded, they are trying to fix the cable, the fiber connection, so kudos to those people are working in very difficult conditions.

There was a call from the Minister of IT from Ukraine to Elon Musk to provide Starlink satellites and dishes, and he sent more than 100 dishes, which is providing some level of connectivity, but of course it's very limited. But maybe it is proving something, that, in areas of war, this technology can be very useful.

Now let's see the other side of the coin, the sanctions on Russia. Again, the Russian Internet is also quite robust. I don't know if you have heard before, but the Russian authorities have, for quite a while now, have started talking about shutting down the Russian Internet, just as an exercise, as a drill. We have only heard rumors of it, but it has never happened, and most probably it never happened because it is very difficult to operate such a shutdown on the Russian Internet.

As you see on this on this graph here, the red dots are local Russian operators, and the blue dots are operators that are outside of Russia. What we see here, there are as many blue dots as red dots, which means that local networks are also connecting to foreign networks in such a way that it would be very difficult to switch off the whole of the Internet. But, what we are also seeing is, there is a concentration on three, maybe four, Russian operators.

But those big operators, they themselves need Internet access, and how they get that Internet access is to talk to the green dots, which are called tier one operators. Tier one operators are -- in a hierarchy, they are topmost ones there. There are a handful of them, maybe we have maybe 10 or 15, but not so many. They are connected to most of the bigger networks of the Internet. What happened on March 4, Lumen and Cogent, which are American companies, decided to stop their service to Russia.

Fine. Which means that Russia cannot access the Internet through those providers, but eventually they will be able to access the Internet through other providers. You have you have many other providers as well. But this can have an impact. For example, it means that Russian networks now have less options to send their traffic abroad, and foreign networks have also less options to conduct Russian networks. Eventually this can have an impact on latency.

The aim of this action was to somehow isolate Russia but, by doing so, you're also isolating a lot of people in Russia who also against the war. So, we need perhaps to strike a balance. Is it good to shut down the Internet even for a country, which is waging war against someone else? Probably not.

What are the impacts of the sanctions? You have big companies, such as Google and Twitter, that have stopped services, maybe for a good reason here, because they do not want, Google or Twitter, for their ad system to be participating to the misinformation campaign by Russian authorities, or by Russian news agencies. We have seen big companies, such as Amazon, Apple, PayPal, Netflix, stopping their services. Even with the banking sanctions, SWIFT is not there anymore, the whole payment system also has stopped functioning. I've heard Russia has moved to UnionPay, which is a Chinese provider of online payment.

On March 11, what happened is the London Internet Exchange Point, which is a very big Internet exchange point, and which has particular members from almost all over the world, they are very popular because the they are connected to the major networks and the major content providers such as Google, Facebook, all of them, they decided to cut the services to two operators, MegaFon and Rostelecom, and we have seen how traffic shifted, because now Russian operators do not have direct access to the set of peers that they usually had before.

Something we also notice is that certification authorities -- so, whenever you visit a website using HTTPS, you have a certificate, these certificates are issued by certificate authorities -- some of them decided to stop the renewal. Let's say you want to go on an e-government service of Russia, you couldn't access it anymore because the certificate expired, and it was not renewed. So, what did the Russians decide to do? They decided, Okay, you guys do not want to renew my certificate, I will create my own certificate authority. They created their own certificate authority. But now, it takes time for a newly created certificate authority to be accepted by browsers, it is a very lengthy process because there's an element of trust and everything. So they say, Okay, if you want now to access to local e-government services, you have to use Russian made browsers. They have a browser called Yandex Browser, which comes pre-installed with a certificate. So, now they are encouraging people in Russia to use their own created browsers to access those local websites,

but this has this has an issue. If someone is providing you a browser with a custom-made certificate, it means that eventually they can also decrypt your traffic, because they are the owner of that root certificate at the end of the day.

The Internet Society has raised red flags many times, including in the case in Mauritius where, at some point, we were discussing about having a proxy server to decrypt traffic, and the way to do that is by installing a certificate in your browser. This is completely bad because it breaks the end-to-end principle of the Internet. It breaks many other principles such as trust, confidentiality, privacy, and so on. So, what we are seeing, by isolating Russia, is that we're encouraging Russia to create what we call the Splinternet, not the Internet, but the Splinternet, which is made of fragments of networks. Sometimes they will be able to connect to each other because they share some common protocols but, in many cases, probably not. We have great examples such as the Great Firewall of China, where they say, Okay, if you stay within the Chinese Internet, you're safe, but we do not know what what's happening behind the doors, and whether there is eavesdropping, state-sponsored surveillance and things like that.

The Internet has succeeded because of its open nature, of its unrestricted access, and the use of common protocols. So, if now the Chinese say they want to build their own, using their own routing protocol, or using, for example, new IP -- they started talking about new IP, which is a completely different set of protocols and not compatible with the current Internet Protocol -- or they decide to install their own DNS root system. This is further fragmenting the Internet, now creating different pieces, fragments, of Internet, and breaking, basically, what we have built, and what we have put so much effort in building a decentralized system of networks of networks.

Therefore, it is important to protect the core properties of the Internet, which are having an accessible infrastructure with a common protocol, the common protocol in our case is TCP/IP, or IP. For the routing protocol, we use BGP which is the common language all network operators we speak. For DNS, everyone knows there is only one root, and we will all use the same root. It must remain decentralized, because it is a network of networks that work independently but, at the end of the day, together. And it needs to stay neutral and a general-purpose Internet, so that anyone can come and add a piece of the Internet, and build Internet, make it grow organic.

Here on the right, you have a set of properties that the Internet needs to be, and we need to fight so that it remains as is, open, reliable, resilient, easy, and with unrestricted access, collaborative, and so on. By refusing access to Russia networks, as we have seen, it crosses out a lot of these critical properties.

So, by the threats, by disconnecting Russia, we are disconnecting the Russian people itself as mentioned. Maybe a big majority of Russian people are against the war, and they need access to information. They need to see how the world is reacting, but the world also needs to have access to what's happening in Russia. Are there protests, or people fighting against this authoritarian regime, so on and so forth? The threat is also that, by disconnecting Russia this is going to set a precedent, and maybe more of this will come, so splintering the Internet along geographical, political, or commercial boundaries.

So, the recommendation is really to resist calls to cut people off the Internet and prioritize action that will help keep the Internet running, even for the Russian people.

This is my final slide about. Andrew Sullivan said that the Internet is allowing people, who would otherwise be silenced, to speak. Also our chair mentioned that, without the Internet, the rest of the world would not know of atrocities happening in other places, and without the Internet, ordinary citizens of many countries wouldn't know what is what was being carried out in their name.

I have put a few references. If you're interested in the more cybersecurity aspects of all the different types of attacks that happen also the mitigation techniques. I'll put the links here. I've also our own analysis, the Internet Society analysis of disconnecting Russia, and so on. On the last link here, we have a rolling blog where we keep putting the latest information about what we see from the networks, either of networks being shut down, or we see a protocol which is no more accessible, or we also work with an organization which works in the space of Internet censorship, so we have live information about which services are being censored in which countries.

That's it. Thank you very much.

Amar Seeam
Do we have any questions?

Any questions from anyone on line?

[Participant]
Can I ask a question?

Amar Seeam
Yes.

[Participant]
How is this going to affect us in Mauritius?

Amar Seeam
The question is how it's going to affect us in Mauritius.

Amreesh Phokeer
Yeah. So, the same considerations. Mauritius, we are also part of the global Internet, and the threats that are there for the global Internet can also happen in Mauritius. I talked about the having a resilient Internet, having multiple connections to other countries. Mauritius being an island, it is important that we have a very robust submarine cable ecosystem, because let's say there is a cable break, it is very easy for Mauritius to go offline. We are almost no more using satellite communications anymore, most of the traffic is going through submarine cables, and we know submarine cables can easily be broken. You have the example of Tonga, which is an island. There was a volcano, the cable broke, and for a lot of time the whole country was out of the Internet.

But this is one, talking about infrastructure, but you have also those threats coming from from policies, whether it is government mandated policies or otherwise. For example, breaking the end-to-end principle of the Internet. Using a proxy server to decrypt traffic is a really bad idea. It undermines the privacy of users, it undermines confidentiality. This can happen anywhere, and it could have happened in Mauritius as well, so we need to be vigilant about how things are evolving.

[Participant]
Okay, thank you. There are many parts of your speech which I really didn't understand, because I'm just a first year cybersecurity student. But, this is a fresh perspective you gave to us, and we have to find out more about all these things. Thank you. Thanks a lot for your presentation.

Amreesh Phokeer
Was a pleasure.

Amar Seeam
Any more questions? Any more uestions from those on campus?

Anywhere online? Yes.

[Participant]
[inaudible] African continent?

Amreesh Phokeer
That's a good question. Of course we have all these economic implications of the war and Russia, where you have surges in the price of gas, for example, and if African countries are importing gas, maybe they would be an increase in the price. But now, thinking of the cyber implications of of this war. We know for a fact that in African countries, there are a lot of [inaudible] authoritarian countries, and there is a trend about Internet shutdowns, either because of war, or even during exam times, some countries will completely just shut down the Internet. So, sanctions, countries in Africa had sanctions before. Sudan, for example, had sanctions from the US.

Maybe this will raise back all these questions, or demons I would say. If now they are applying sanctions on the Internet for Russia, would they apply sanctions on the Internet for African countries. We know for a fact that, in many African countries, access to the Internet is limited, or actually already costly, so sanctions on African countries will make the situation even worse for the locals.

Amar Seeam
One more question, yes. ,

Amreesh Phokeer
What I've read is that the Russian cyber criminals are not only attacking Ukraine to to shut down the Internet, but they're also attacking allies between, so NATO countries. You might have heard, I think it was during the US presidential election, how Russians influenced the elections. So, cybercriminals can have actually quite large influence on things that you might not be thinking of, so that's why it's important for countries to be aware of those cyber attacks, and how to put all the mitigation around it to reduce the effect.

[Participant]
[inaudible]

Amar Seeam
Any further questions?

On just maybe the importance of routing security, maybe talk a bit more about that, and some of the things that Internet Society are doing?

Amreesh Phokeer
Yeah, yeah, sure. That's a good example, because yesterday itself, Twitter was hijacked in Russia. What happened is that, obviously maybe for reasons that we all know, they do not want the Russian population to have access to Twitter. So, they decided to block Twitter, so the big red operators, the red circles we have seen, decided to block Twitter. The way they do that is -- the way the Internet works on a protocol called BGP, which a network says, I am network X, come, send your traffic to me. So, what happened is that the Russian network said, I am Twitter, send your traffic to me, and then they would they would blackhole the traffic, so that users in Russia cannot access to Twitter.

But what happened is they also leaked that, what we call that announcement, to many places on the Internet, and a lot of neighboring countries, for example, could get access to that during that short span of time. But, at the Internet Society, we have a program called MANRS, which is Mutually Agreed Norms on Routing Security, in which we try to push for the best practices in terms of routing security, or RPKI, Resource Public Key Infrastructure. Actually Twitter is using this type of technology, which is cryptography supported technology, so, thanks to that, the outage on Twitter wasn't that big. Maybe 10 or 12 years ago, there was a very similar incident with Pakistan telecom trying to block YouTube. They did the exact same thing, they hijacked the YouTube network, and said that, if you want to access YouTube, come to my network, and this is what happened, but there was a leak. They leaked that announcement and it went around the world, and I think the whole of Asia couldn't access YouTube for one or two hours.

So, thanks to the routing security mechanisms that we at the Internet Society are pushing for adoption, Twitter was able to mitigate this this action,

Amar Seeam
Thank you.

Any further questions anyone online?

Okay, thanks so much for your presentation.

So, now we're going to move on to the next segment of the session, which is short membership talk from the Branch. So, I'd like to invite the Branch to come up and give us a short talk on membership for anyone who is interested in joining the IEEE.

[Participant]
Hello, everyone. My name is [inaudible]. I'm the secretary of the Student Branch and I would like to talk to you about the advantages of entering the IEEE Student Branch Society. First of all, we have free access to IEEE resources online, Google Apps @ IEEE, IEEE mini labs, invitation to attend global talks and events, professional networking, potential magazine, student travel grants, free access to Cisco Academy courses with certificates of completion, with no additional costs, and participate in organizing major events.

[Participant]
Hello, everyone. My name is [inaudible], the Treasurer of the Society. I will tell you how to join the society. First of all you have to go to the IEEE website and click on Join as Student. You'll then be prompted to create an account if you don't have one. You create your account and proceed to Step three. If you already have an account, you can sign in and proceed to Step three. You fill the forms and ensure that you choose Middlesex University Mauritius as university name. iIf you're unsure, please contact any other current branch executive members. You proceed with the payment. The fee is usually $27 but if you enter the FUTURE50 s athe promo code you will only pay $13:50 approximately 600 rupees, which is fairly cheap as subscription fee for all the benefits mentioned above. You then send an email to the secretary direct and notify him about your subscription. Thank you.

Elnathan Vally
We are going to, if you want to join the society, we are going to collect your names and then will revert back to you on a written description on how to join the society. We have already collected a list of who registered for the webinar, so, in a short while, we will send you back an email to guide you on the steps of joining the society, and you're membership payment. Thank you

Amar Seeam
That bring brings us to the course of this session. We do have one more webinar at the end of this week, slightly different. We're looking at modeling the the ,marine ecosystem of Mauritius, specifically looking at the effects of the oil spill. So, that's for anyone who's interested in this specific area, we'll be having that this Friday, and the register link is down there below. cybermdx.cloud/marine.

We thank you once more for joining us for such an excellent talk on the Cybersecurity of the Russia Ukraine Conflict. We will be having more talks and cybersecurity if that interests you. We'll be having one that joins both of the marine and cybersecurity sides, there is one coming up that looks at the cybersecurity of the marine industry and shipping logistics and all those kind of things. So, that's coming up soon.

So thanks one more, and thanks again to Dr. Amreesh for his excellent talk, and thanks to the Branch for organizing this event, and we'll hope to see some more of you at subsequent events that we hold. So, bye for now. that brings us to the end of the seminar.